CLAIMS

1. A method of preparing a document so that it can be authenticated; comprising the following steps:

(a) selecting data sufficient to authenticate the document;

(b) generating a cryptographic key to encode the selected data;

(c) encoding the cryptographic key so that it forms a digital representation of a graphic image; and

(d) printing the graphic image on the document.

2. The method of Claim 1 comprising the steps of encoding the selected data using the cryptographic key and then printing the encoded, selected data on the document.

3. The method of Claim 2 comprising the step of scanning the graphic image to extract the key in order to use the key to encode the selected data.

4. The method of Claim 2 comprising the step of looking up the key in a database and then encoding the selected data using that key.

5. The method of any preceding Claim 2 – 4 in which the encoded, selected data can be generated by hashing or encryption using the key.

6. The method of Claim 1 in which the selected data comprises data that is printed on the document in a human readable or machine readable form.

7. The method of Claim 1 comprising the further step of (a) encoding the selected data by encrypting or hashing the selected data using the key derived or derivable from the graphic image printed onto the document; (b) printing the encrypted or hashed selected data as text or a graphic on the document.

8. The method of any preceding claim in which, when the document has to be authenticated, the document is scanned to automatically extract the key by a scanner.

16. The method of any preceding claim in which the graphic is a one or two dimensional bar-code or other graphical symbol.

17. The method of Claim 16 in which the graphic image is a two dimensional graphical symbol and the external shape of the graphic image can be adapted so that it is visually compatible with other images on the document.

18. The method of Claim 17 in which the appearance of the graphic image can be adapted so that it is visually compatible with other images on the document.

19. The method of any preceding Claim in which the document is any object that can carry a printed image.

20. The method of Claim 15 in which the document is a check.

21. The method of any preceding Claim in which a step of authentication occurs at a check cashing outlet, bank of first deposit or point of sale.

22. The method of Claim 15 in which the document is printed packaging.

23. A document prepared according to the method of any preceding Claim 1 – 22.

9. The method of Claim 8 as dependent on any Claims 2 – 7, in which the key extracted by scanning enables authentication because the method comprises the further steps of (a) using the extracted key to encode the selected data printed on the document and (b) automatically comparing the result with the encoded, selected data printed onto the document.

10. The method of preceding Claim 9 in which the extracted key is not explicitly revealed at any time but instead fed directly to an algorithm used to encode the selected data printed on the document.

11. The method of Claim 8 in which the key automatically extracted by scanning enables authentication because it is a personal identification number and the method comprises the further step of requiring an end-user to enter his personal identification number at a terminal and automatically comparing that number with the number automatically extracted from the scanned graphic.

12. The method of any preceding Claim in which different keys are automatically generated for different documents.

13. The method of any preceding Claim in which the key is generated by a random process or other non-sequential method that makes it difficult to link the key to any data encoded on the document.

14. The method of any preceding Claim in which an algorithm is used to decode the key as part of the authentication process and the method comprises the further step of amending the parameters of the algorithm to enhance security.

15. The method of preceding Claim 14 in which parameters needed to decode the key are downloaded to the location at which document authentication is to occur at widely spaced intervals of time and not for each successive document.